ITRM Policy SEC500-02
Date: July 1, 2006

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Technology Security Policy

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Associate Director for Policy Practice and Architecture (PPA) within the Technology Strategies and Solutions (TSS) Directorate. PPA will issue a Change Notice Alert and post on the VITA Web site, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers to be interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	1990	Base Document: COV ITRM Policy 90.1 Information Technology Security Policy
Revision 3	12/07/2001	Revision to align with current information security best practices.
Revision 4	07/01/2006	Revision to align with changes to the *Code of Virginia*, and with SEC501-01.

PREFACE

Publication Designation
ITRM Policy SEC500-02

Subject
Information Technology Security Policy

Effective Date
July 1, 2006

Compliance Date
July 1, 2007

Supersedes
COV ITRM Policy 90.1 Information Technology Security Policy, dated December 7, 2001

Scheduled Review
Council of Technology Services
One (1) year from effective date

Authority
Code of Virginia, § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA"; Appointment of Chief Information Officer [CIO])

Code of Virginia, §2.2-2827
(Restrictions on state employee access to information infrastructure)

Code of Virginia, §2.2-3800
(Government Data Collection and Dissemination Practices Act)

Scope
This policy is applicable to all State agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology resources in the Commonwealth. However, academic "instruction or research" systems are exempt from this policy provided they are not subject to a State or Federal Law/Act mandating security due diligence. This policy is offered only as guidance to local government entities.

Purpose
To protect the Commonwealth information technology assets and the information processed by defining the minimum information technology security program for agencies of the Commonwealth of Virginia (COV).

General Responsibilities
(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer of the Commonwealth

In accordance with *Code of Virginia*, § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits."*

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures and standards to protect the confidentiality, integrity, and availability of the Commonwealth's information assets.

Council on Technology Services
In accordance with the *Code of Virginia* § 2.2-2009, the Council on Technology Services is assigned the following duties: "*In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services."*

Technology Strategies and Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Technology Strategies and Solutions Directorate the following duties: "*Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

All State Agencies
In accordance with the *Code of Virginia* § 2.2-603, § 2.2-2009, and § 2.2-2010 all State Agencies are responsible for complying with Commonwealth ITRM policies and standards and considering Commonwealth ITRM guidelines issued by the CIO. In addition: "*The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence."*

Regulatory References
1. Health Insurance Portability and Accountability Act.
2. Privacy Act of 1974.
3. Children's Online Privacy Protection Act.
4. Family Educational Rights and Privacy Act.
5. Executive Order of Critical Infrastructure Protection.
6. Federal Child Pornography Statute: 18 U.S.C. & 2252

7. Bank Secrecy Act.
8. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3, .4, .5, and .6.
9. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85.
10. Federal Information Security Management Act (FISMA).
11. Office of Management and Budget (OMB) Circular A-130.

International Standards

1. International Standard, Information Technology – code of practice for information security management, BS ISO/IEC 17799:2005.

Definitions

See Glossary

Related ITRM Standard

ITRM Standard SEC501-01: Information Technology Security Standard (Revised July 1, 2006)

TABLE OF CONTENTS

1. INFORMATION TECHNOLOGY (IT) SECURITY POLICY STATEMENT

1.1 Background

The Commonwealth of Virginia (COV) relies heavily on the application of information technology (IT) for the effective delivery of government services. Rapid and continuing technical advances have increased the dependence of COV agencies on IT. COV data, software, hardware, and telecommunications are recognized by Agencies as important resources and must be protected through Agency IT security programs.

Agency IT security programs shall be built on the concept of public trust. An Agency IT security program provides sustainability — a consistent approach to IT security that can be replicated across networks, applications, and transactions. The COV IT Security Program provides the generally acceptable principles and practices for Agencies to use in securing their IT systems and data.

1.2 Guiding Principles

The following principles guide the development and implementation of the COV IT Security Program.

a. COV Data is:

   1. A critical asset that shall be protected;

   2. Restricted to authorized personnel for official use.

b. IT security must be:

   1. A cornerstone of maintaining public trust;

   2. Managed to address both business and technology requirements;

   3. Risk-based and cost-effective;

   4. Aligned with COV priorities, industry-prudent practices, and government requirements;

   5. Directed by policy but implemented by business owners;

   6. The responsibility of all users of COV IT systems and data.

1.3 Statement of Policy

It remains the policy of the COV that each Agency Head is responsible for the security of the Agency's data and for taking appropriate steps to secure Agency IT systems and data through the development of an Agency IT security program as stated both in this policy and the superseded policy Information *Technology Security Policy* (COV ITRM Policy 90-1).

This policy and related standards provide the minimum requirements for each COV Agency's IT security program to be implemented in a framework relative to information risk. Agency Heads

may establish additional, more restrictive IT security programs and related policies but must, at a minimum, meet the requirements of this policy and the related standards. If, in the sole judgment of the Agency Head, the Agency cannot meet one or more of the minimum requirements, a request for an exception shall be made in writing to the Chief Information Security Officer of the Commonwealth (CISO) for consideration. This process is described in more detail in Section 7 of this document, as well as in Section 1.5 of the *Information Technology Security Standard* (COV ITRM Standard 501-01). The form that an Agency must submit to request an exception to any requirement of this policy or the related Standards is attached as the Appendix to this document.

The function of this policy is to protect COV IT systems and data from credible threats, whether internal or external, deliberate or accidental. It is the policy of COV to use all reasonable IT security control measures to:

a. Protect COV data against unauthorized access and use;

b. Maintain integrity of COV data;

c. Meet requirements for availability of data residing on IT systems;

d. Meet federal, state and other regulatory and legislative requirements.

The remainder of this policy is divided into seven sections that define the requirements for each Agency's IT security program.

a. Section 2 addresses key roles and responsibilities of managers to provide IT security measures and controls to protect the COV IT systems and data.

b. Section 3 addresses the COV IT Security Program and outlines the IT security subprograms.

c. Section 4 addresses IT security compliance and proper administration of the COV IT Security Program with program management oversight.

d. Section 5 addresses IT security audits to test for adequacy of controls and assess the level of compliance with established policies, standards, or procedures. Section 5 also summarizes the *IT Security Audit Standard* (COV ITRM Standard SEC507-00) which provides specific IT security audit requirements for Agencies, which are summarized in this section.

e. Section 6 defines COV policy for the confiscation and removal of IT resources.

f. Section 7 describes the process for requesting an exception to the requirements of this policy and the related standards.

g. Section 8 contains a glossary of IT security definitions.

h. Section 9 contains a list and description of IT security acronyms and the terms to which they refer.

2. KEY IT SECURITY ROLES AND RESPONSIBILITIES

IT security roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Additional information concerning the assignment of multiple IT security roles is contained in section 2.2 of the *IT Security Standard* (COV ITRM Standard SEC501-01).

2.1 Chief Information Officer of the Commonwealth (CIO)

The *Code of Virginia* §2-2.2009 states that *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications."*

2.2 Chief Information Security Officer (CISO)

The CISO is responsible for development and coordination of the COV IT Security Program and, as such, performs the following duties:

a. Administers the COV IT Security Program and periodically assesses whether the program is implemented in accordance with COV IT Security Policies and Standards.

b. Reviews requested exceptions to COV IT Security Policies, Standards and Procedures.

c. Provides solutions, guidance, and expertise in IT security.

d. Maintains awareness of the security status of sensitive IT systems.

e. Facilitates effective implementation of COV IT Security Program, by:

   i. Preparing, disseminating, and maintaining IT security, policies, standards, guidelines and procedures as appropriate;
   ii. Collecting data relative to the state of IT security in the COV and communicating as needed;
   iii. Providing consultation on balancing an effective IT security program with business needs.

f. Provides networking and liaison opportunities to Information Security Officers (ISOs).

2.3 Agency Head

Each Agency Head is responsible for the security of the Agency's IT systems and data. The Agency Head's IT security responsibilities include the following:

a. Designate via e-mail to VITASecurityServices@vita.virginia.gov an ISO for the Agency and providing the person's name, title and contact information to VITA no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO, as well.

b. Determine the optimal place of the IT security function within the Agency hierarchy with the shortest practicable reporting line to the Agency Head.

c. Maintain an Agency IT security program that is sufficient to protect the Agency's IT systems, and that is documented and effectively communicated.

d. Review and approve the Agency's Business Impact Analyses (BIAs), a Risk Assessment (RA), and a Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.

e. Accept residual risk as described in section 2.5 of the *IT Security Audit Standard* (COV ITRM Standard SEC507-00).

f. Maintain compliance with *IT Security Audit Standard* (COV ITRM Standard SEC507-00). This compliance must include, but is not limited to:

- Requiring development and implementation of an Agency plan for IT security audits, and submitting this plan to the CISO;
- Requiring that the planned IT security audits are conducted;
- Receiving reports of the results of IT security audits;
- Requiring development of Corrective Action Plans to address findings of IT security audits; and
- Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings. .

g. Facilitate the communication process between data processing staff and those in other areas of the Agency.

h. Establish a program of IT security safeguards.

i. Establish an IT security awareness and training program.

j. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

Managers in all Agencies and at all levels shall provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

2.4 Information Security Officer (ISO)

The ISO is responsible for developing and managing the Agency's IT security program. The ISO's duties are as follows:

a. Develop and manage an Agency IT security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.

b. Develop and maintain an IT security awareness and training program for Agency staff,

including contractors and IT service providers.

c. Coordinate and provide IT security information to the CISO as required.

d. Implement and maintain the appropriate balance of protective, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality.

e. Mitigate and report all IT security incidents in accordance with §2.2-603 of the *Code of Virginia* and VITA requirements and take appropriate actions to prevent recurrence.

f. Maintain liaison with the CISO.

2.5 Privacy Officer

An Agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise these responsibilities are carried out by the ISO. The Privacy Officer provides guidance on:

a. The requirements of state and federal Privacy laws.

b. Disclosure of and access to sensitive data.

c. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

2.6 System Owner

The System Owner is the Agency manager responsible for operation and maintenance of an Agency IT system. With respect to IT security, the System Owner's responsibilities include the following:

a. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.

b. Manage system risk and developing any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.

c. Maintain compliance with COV IT security policies and standards in all IT system activities.

d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

e. Designate a System Administrator for the system.

2.7 Data Owner

The Data Owner is the Agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

a. Evaluate and classify sensitivity of the data.

b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

c. Communicate data protection requirements to the System Owner.

d. Define requirements for access to the data.

2.8 System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists Agency management in the day-to-day administration of Agency IT systems, and implements security controls and other requirements of the Agency IT security program on IT systems for which the System Administrator have been assigned responsibility.

2.9 Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.

b. Establish, monitoring, and operating IT systems in a manner consistent with COV IT security policies and standards.

c. Provide Data Owners with reports, when necessary and applicable.

2.10 IT System Users

All users of COV IT systems including employees and contractors are responsible for the following:

a. Read and comply with Agency IT security program requirements.

b. Report breaches of IT security, actual or suspected, to their agency management and/or the CISO.

c. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

3. IT SECURITY PROGRAM

The CISO is charged with developing and administering the COV IT Security Program. The Agency ISO is charged with developing and administering the Agency IT security program in a manner that

meets Agency business needs, protects IT systems and data in a manner commensurate with data sensitivity and risk, and, at a minimum, meets the requirements of COV policies and standards.

3.1 IT Security Program Components

The policy of the COV is to secure its IT systems using methods based on the sensitivity of the data processed and the risks to which the systems and data are subject, including the dependence of critical Agency business processes on the data and systems.

Figure 1 (shown on the next page to improve its legibility) illustrates the process by which the COV IT Security Program components interact to enable COV Agencies to accomplish their missions in a safe and secure technology environment.

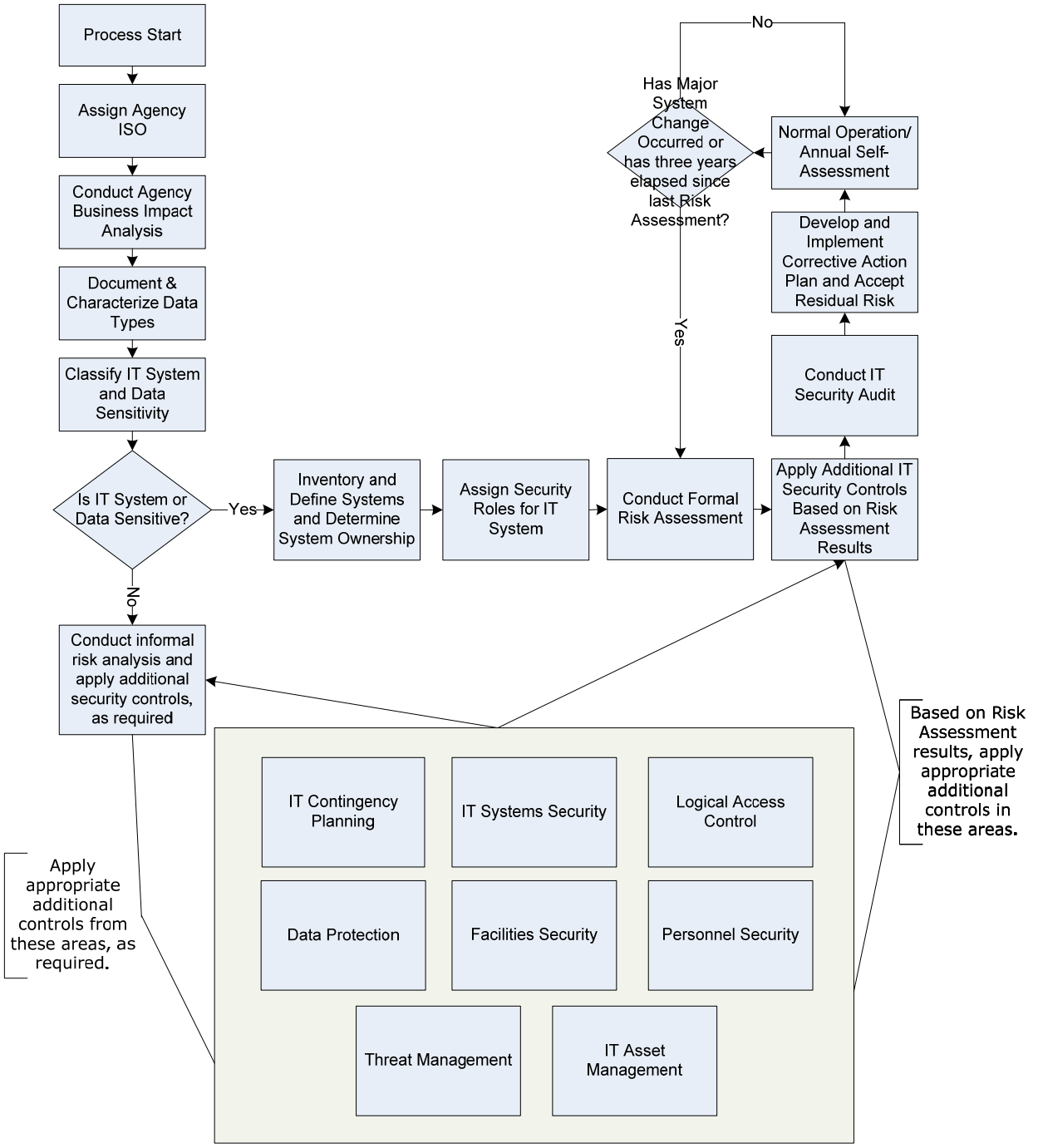

Figure 1 - Commonwealth of Virginia IT Security Framework

The components of this framework provide the basis for designing the Agency's IT security program and safeguards. They do not represent organizational functions within the IT security program, but rather the functional components of the IT security program.

3.1.1 Risk Management

As previously stated, this policy and related standards are based on protecting COV IT systems and data based on sensitivity and risk, including system availability needs. Accordingly, Risk Management is a central component of an Agency IT security program and allows each Agency to determine how these factors apply to its IT systems.

The first step in Risk Management is a BIA. BIA is a process of analyzing Agency business functions, to identify those that are essential or those that contain sensitive data, and assessing the resources that support them. For the purposes of IT security, the BIA identifies those business functions that are essential or involve sensitive data and that are dependent on IT. This analysis is necessary in order to determine the appropriate level of protection for IT systems and the data they process.

After completing the BIA, Agencies document and characterize the types of data they handle, and classify the sensitivity of Agency IT systems and data for use in the RA process. Sensitivity must consider the elements of availability, confidentiality and integrity.

Agencies then define, inventory, and determine ownership of all Agency IT systems classified as sensitive so that IT security roles can be appropriately assigned.

A periodic, formal RA is required for all Agency IT systems classified as sensitive. While a formal RA is not required for IT systems that are not sensitive, Agencies are advised to conduct an informal risk analysis on those IT systems and the data they handle, and to apply appropriate additional IT security controls as required. The RA process assesses the threats to Agency IT systems and data, probabilities of occurrence and the appropriate IT security controls necessary to reduce these risks to an acceptable level.

After appropriate mitigating IT security controls have been applied relative to sensitivity and risk, based on RA results, sensitive Agency IT systems require periodic, independent IT Security Audits. These audits are necessary to determine whether the overall protection of Agency IT systems and the data they handle is adequate and effective. The requirements for IT Security Audits are discussed in more detail in Section 5 of this document, and in the *IT Security Audit Standard* (COV ITRM Standard SEC507-00).

IT Security Audits may identify additional required mitigating controls for sensitive Agency IT systems in order to provide adequate and effective protection of the systems and the data they handle. After applying these controls, the final step in the Risk Management process is formal acceptance by the Agency Head or designee of any residual risk to Agency operations from sensitive Agency IT systems.

3.1.2 IT Contingency Planning

IT Contingency Planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and data that support essential business functions if an event occurs that renders the IT systems and data unavailable. IT Contingency Planning includes Continuity of Operations Planning, Disaster Recovery Planning, and IT System Backup and Restoration.

A key element of IT contingency planning is Continuity of Operations Planning, which provides a business continuation strategy for essential Agency business functions as

identified in the BIA. These processes may or may not be dependent on IT resources. The Virginia Department of Emergency Management (VDEM) provides the COV guidance on Agency Continuity of Operations Plans.

Disaster Recovery Planning supports Continuity of Operations Planning by defining specific policies, processes, standards, and procedures for restoring IT systems and data that support essential business functions, on a schedule that supports Agency mission requirements.

Based on related elements in the IT contingency planning process, IT System Backup and Restoration defines plans and restoration schedules that meet Agency mission requirements for the backup and restoration of data.

3.1.3 IT Systems Security

The purpose of IT systems security is to define the steps necessary to provide adequate and effective protection for Agency IT systems in the areas of IT System Hardening, IT Systems Interoperability Security, Malicious Code Protection, and IT Systems Development Life Cycle Security. Agency IT systems may require further security controls for adequate protection based on the identification of sensitivity and risk to these systems, including system availability needs, identified through Risk Management policies, processes, and procedures. In addition, some security controls are necessary independent of sensitivity and risk.

3.1.4 Logical Access Control

Logical Access Control requirements define the steps necessary to protect the confidentiality, integrity, and availability of COV IT systems and data against compromise. Logical Access Control requirements identify the measures needed to verify that all IT system users are who they say they are and that they are permitted to use the systems and data they are attempting to access. Logical Access Control defines requirements in the areas of Account Management, Password Management, and Remote Access.

3.1.5 Data Protection

Data Protection provides security safeguards for the processing and storing of data. This component of the COV IT Security Program outlines the methods that Agencies can use to safeguard the data in a manner commensurate with the sensitivity and risk of the data stored. Data Protection includes requirements in the areas of Media Protection and Encryption.

3.1.6 Facilities Security

Facilities Security safeguards require planning and application of facilities security practices to provide a first line of defense for IT systems against damage, theft, unauthorized disclosure of data, loss of control over system integrity, and interruption to computer services.

3.1.7 Personnel Security

Personnel Security controls reduce risk to COV IT systems and data by specifying Access Determination and Control requirements that restrict access to these systems and data to those individuals who require such access as part of their job duties. Personnel Security also

includes Security Awareness and Training requirements to provide all IT system users with appropriate understanding regarding COV IT security policies and Acceptable Use requirements for COV IT systems and data.

3.1.8 Threat Management

Threat Management addresses protection of COV IT systems and data by preparing for and responding to IT security incidents. This component of the COV IT Security Program includes Threat Detection, Incident Handling, and IT Security Monitoring and Logging.

3.1.9 IT Asset Management

IT Asset Management concerns protection of the components that comprise COV IT systems by managing them in a planned, organized, and secure fashion. Asset Management includes IT Asset Control, Software License Management, and Configuration Management and Change Control.

4. COMPLIANCE

The COV measures compliance with IT security policies and standards through processes that include, but are not limited to:

- inspections, reviews, and evaluations;
- monitoring;
- audits; and
- confiscation and removal of IT systems and data.

4.1 Monitoring

4.1.1 General Monitoring Activities

Monitoring is used to improve IT security, to assess appropriate use of COV IT resources, and to protect those resources from attack. Use of COV IT resources constitutes permission to monitor that use. There is no expectation of privacy when utilizing COV IT resources. The COV reserves the right to:

a. Review the data contained in or traversing COV IT resources.

b. Review the activities on COV IT resources.

c. Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the CIO.

4.1.2 User Agreement to Monitoring

Any use of COV IT resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of COV IT resources:

a. Agree to comply with COV policy concerning the use of IT resources;

b. Acknowledge that their activities may be subject to monitoring;

c. Acknowledge that any detected misuse of COV IT resources may be subject to disciplinary action and legal prosecution.

4.1.3 Internet Privacy

The *Code of Virginia* § 2.2-3803 (B) requires every public body in the COV that has an Internet website to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the requirements of the *Code*.

4.1.4 User Monitoring Notification

Where possible, all IT system users will be notified by the display of an authorized COV warning banner that COV IT systems may be monitored and viewed by authorized personnel, regardless of privacy concerns. This notice shall, at a minimum, appear whenever the IT system user first logs on to the IT system and shall be included in IT security awareness training.

4.1.5 What is Monitored?

Monitoring of COV IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes and user commands; e-mail and Internet usage; and message and data content.

4.1.6 Requesting and Authorizing Monitoring

The CISO or ISO when appropriate has the responsibility to authorize monitoring or scanning activities for network traffic, application and data access, keystrokes, user commands, and e-mail and Internet usage for COV IT systems and data. The CISO and the ISO shall notify each other when appropriate.

4.1.7 Infrastructure Monitoring
Agency IT personnel are responsible for maintaining security in their environment through the following processes:

a. Monitoring all systems for security baselines and policy compliance.

b. Notifying the CISO and Agency ISO of any detected or suspected incidents.

c. Monitoring their environment infrastructure.

d. Installing or using unauthorized monitoring devices is strictly prohibited.

5. IT SECURITY AUDITS

5.1 Description

The Code of Virginia § 2.2-2009 gives the CIO the responsibility to *"direct the development of policies, procedures and standards for . . . performing security audits of government databases and*

data communications." These policies are outlined in this section; specific requirements are detailed in the *IT Security Audit Standard* (COV ITRM Standard SEC507-00).

5.2 Performance of IT Security Audits

As required by the *IT Security Audit Standard* (COV ITRM Standard SEC507-00), IT Security Audits (audits) shall be conducted by CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

Annually, each Agency is required to develop and submit to the CISO an audit plan for Agency government databases. Strictly speaking, a government database is a collection of COV data organized into interrelated tables and specifications of data objects.

For the purposes of this standard, however, the term "government database" shall include all components of any COV IT system in which a database resides, and shall also include state Data Communications, as defined below. This definition of "government database" applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental.

Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of information. As used in this section, Data Communications is included in the definition of government database, herein.

The audits conducted under the annual Agency audit plan must measure compliance with this *Information Technology Security Policy* (COV ITRM Policy SEC500-02) and the *Information Technology Security Standard* (COV ITRM Standard SEC501-01). IT Security Auditors also should also use standards that measure compliance with any other applicable federal and COV regulations.

5.3 Documentation and Reporting of IT Security Audits

After conducting the audit, the auditor shall report the audit results to the Agency Head. The Agency Head shall then require the development of a Corrective Action Plan that includes concurrence or non-concurrence with each finding in the audit report as well as the mitigation strategies. At least once each quarter, each Agency Head or designee shall submit to the CISO a report containing a record of all IT Security Audits conducted by or on behalf of the Agency during that quarter. The report must include all findings and specify whether the Agency concurs or does not concur with each. The report must also include the status of outstanding corrective actions for all IT Security Audits previously conducted by or on behalf of the Agency.

6. PROTECTION OF IT RESOURCES

6.1 Confiscation and Removal of IT Resources

The CISO, in conjunction with the Agency Head through the Agency ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of COV IT security laws or policies to preserve evidence that might be utilized in forensic analysis of a security incident.

7. PROCESS FOR REQUESTING EXCEPTION TO IT SECURITY POLICY

If an Agency Head determines that compliance with the provisions of this *ITRM Information Technology Security Policy* (COV ITRM Policy SEC500-02) or related standards would result in a significant adverse impact to the Agency, the Agency Head may request approval to deviate from that security policy requirement by submitting an exception request to the CISO (see the form attached as the Appendix to this document).

Each request shall be in writing to the CISO from the Agency Head. Included in each request shall be a statement detailing the reasons for the exception and compensating controls. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken. Denied exception requests may be appealed to the CIO of the Commonwealth through the CISO.

8. GLOSSARY OF IT SECURITY DEFINITIONS

Academic Instruction and Research Systems: Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

Access: The ability or permission to enter or pass through an area or to view, change, or communicate with an IT system.

Access Controls: A set of procedures performed by hardware, software, and administrators to monitor access, identify all IT system users requesting access, record access attempts, and prevent unauthorized access to IT systems and data. Account an established relationship between a user and an IT system.

Accountability: The association of each log-on ID with one and only one user, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.

Agency Head: The chief executive officer of a department established in the executive branch of the Commonwealth of Virginia.

Alert: Advance notification that an emergency or disaster situation may occur.

Alternate Site: A location used to conduct critical business functions in the event that access to the primary facility is denied or the primary facility has been so damaged as to be unusable.

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System.*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application, Support System,* and *Information Technology (IT) System.*

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Attack: An attempt to bypass security controls on an IT system. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT system and the effectiveness of existing countermeasures.

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Authenticate: To determine that something is genuine. To reliably determine the identity of a communicating party or device.

Authentication: The process of verifying the identity of a station, originator, or individual to determine the right to access specific types of data. In addition, a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator. During the process, the user enters a name or account number (identification) and password (authentication).

Authenticator: The material or credential used to create or implement authentication bindings such as a password, PIN number, token seed, smart card seed, etc.

Authorization: Granting the right of access to a user, program, or process. The privileges granted to an individual by a designated official to access data, based upon the individual's job, clearance, and need to know.

Availability: The computer security characteristic that addresses requirements for IT systems and data to be operational in support of essential business functions and that measures the sensitivity of IT systems and data to unexpected outages.

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

Baseline Security Configuration: The minimum set of security controls that must be implemented on all IT systems of a particular type.

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function.*

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions.

Chain of Custody: Documentation that is sufficient to prove continuous and unbroken possession of a confiscated IT system.

Change Control: A management process to provide control and traceability for all changes made to an application system or IT system.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data.

Commonwealth of Virginia (COV): The Executive Branch of the government of the Commonwealth of Virginia, or its Agencies or departments.

Computer Emergency Response Team Coordination Center (CERT/CC): a center of Internet security expertise, located at the Software Engineering Institute at Carnegie Mellon University that studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to assist the CERTs of other organizations. See also *Incident Response Team* and *United States Computer Emergency Response Team (US-CERT).*

Confidentiality: The computer security characteristic that addresses requirements that data is disclosed only to those authorized to access it, and that measures the sensitivity of data to unauthorized disclosure.

Configuration Management: A formal process for authorizing and tracking all changes to both hardware and software of an IT system during its life cycle.

Continuity of Operations Planning: The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.
Continuity of Operations Plan (COOP): A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

Control Objectives for Information and related Technology (COBIT): A framework of best practices (framework) for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

Council on Technology Services (COTS): An advisory council that assists in the development of a blueprint for state government IT planning and decision-making. The Council advises the Chief Information Officer of the Commonwealth on the services provided by the Virginia Information Technologies Agency (VITA) and the development and use of applications in state agencies and public institutions of higher education.

Countermeasure: An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an IT system.

Credential: Information passed from one entity to another that is used to establish the sending entity's access rights.

Data: Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge.

Database: A database is a collection of data organized into interrelated tables and specifications of data objects.

Data Classification: A process of categorizing data according to its sensitivity.

Data Communications: Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate Commonwealth of Virginia (COV) data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information. As used in this document, Data Communications is included in the definition of government database, herein.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An Agency Manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Disaster Recovery Plan (DRP): A set of documented procedures that identify the steps to restore essential business functions on a schedule that supports Agency mission requirements.

Data Storage Media: A device used to store IT data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Encryption: A means of scrambling data so it cannot be read without the appropriate decryption methodology.

Essential Business Function: A business function is essential if disruption or degradation of the function prevents the Agency from performing its mission as described in the Agency mission statement.

Evaluation: Investigative and test procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Extranet: A trusted network; used by COV to connect to a third-party provider.

Federal Information Security Management Act (FISMA): Federal legislation whose primary purpose is to provide a comprehensive framework for IT security controls in Federal agencies.

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Function: A purpose, process, or role.

Government Database: For the purposes of this document, the term "government database" includes both databases that contain COV data and data communications that transport COV data. This definition applies irrespective of whether the COV information is in a physical database structure maintained by COV or a third-party provider. However, this definition does not include databases within Agencies that have been determined by the Agencies themselves to be non-governmental. See also *Database* and *Data Communications.*

Group: A named collection of IT system users; created for convenience when stating authorization policy.

Harden: The process of implementing software, hardware, or physical security controls to mitigate risk associated with COV infrastructure and/or sensitive IT systems and data.

High Availability: A requirement that the IT system is continuously available, has a low threshold for down time, or both.

Identification: The process of associating a user with a unique user ID or login ID.

Incident Response Capability (IRC): The follow-up to an unplanned event such as a hardware or software failure or attack against a computer or network.

Incident Response Team: An organization within an Agency constituted to monitor IT security threats and prepare for and respond to cyber attacks. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *United States Computer Emergency Response Team (US-CERT).*

Individual Accountability: The process of associating one and only one IT system user or IT system (such as a workstation or terminal) with any actions performed.

Information Security Officer (ISO): The individual who is responsible for the development, implementation, oversight, and maintenance of the Agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Infrastructure Library (ITIL): A framework of best practice processes designed to facilitate the delivery of high quality information technology (IT) services.

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data.

Information Technology (IT) Security Audit: An independent review and examination of an IT system's policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Auditor: CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT security audits.

Information Technology (IT) Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system. These mechanisms may include but are not necessarily limited to: hardware and software security features; operating procedures, authorization and accountability access and distribution practices; management constraints; personnel security; and environmental and physical safeguards, structures, and devices. Also called IT security safeguards and countermeasures.

Information Technology (IT) Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system. A security incident includes an attempt to violate an explicit or implied security policy.

Information Technology (IT) Security Logging: Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Information Technology (IT) Security Requirements: The types and levels of protection necessary to adequately secure an IT system.

Information Technology (IT) Security Safeguards: See *Information Technology (IT) Security Controls.*

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System.*

Information Technology (IT) System Users: As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of COV IT systems, applications, telecommunication networks, data, and related resources. It excludes customers whose only access is through publicly available services, such as public COV Web sites.

Insecure: Unprotected, as an IT system.

Integrity: The computer security characteristic that addresses the accuracy and completeness of IT systems and data, and that measures the sensitivity of IT systems and data to unauthorized or unexpected modification.

Integrity Check: Validates that a message has not been altered since it was generated by a legitimate source (based on representation of information as numbers and mathematic manipulation of those numbers).

Internet: An external worldwide public data network using Internet protocols to which COV can establish connections. COV has no control over the Internet and cannot guarantee the confidentiality, integrity, or availability of its communications.

Intranet: A trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet protocols, which can be developed, operated and maintained for the conduct of COV business.

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software expert systems.

Intrusion Detection Systems (IDS): Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS): Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

ISO/IEC 17799: An IT security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

Key: A sequence of data used in cryptography to encrypt or decrypt information. The keys must be known or deduced to forge a digital signature or decrypt an encrypted message.

Key Escrow: The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IT system.

Log: To record an action.

Log File: A chronological record of operational and security-related events that have occurred.

Logon ID: An identification code (normally a group of numbers, letters, and special characters) assigned to a particular user that identifies the user to the IT system.

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses (boot sector, file infector, multipartite, link, stealth, macro, e-mail, etc.), Trojan horses, trap doors, worms, spyware, and counterfeit computer instructions (executables).

Malicious Software: See Malicious Code.

Mission Critical Facilities: The data center's physical surroundings as well as data processing equipment inside and the systems supporting them that need to be secured to achieve the availability goals of the system function.

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

Non-sensitive Data: Data of which the compromise with respect to confidentiality, integrity, and/or availability could not adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

Off-site Storage: The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be at least 500 yards from the primary site and offer environmental and physical access protection.

Operational Risk: Any risk that is not market risk or credit risk related. This includes the risk of loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes. Examples of operational risk include: technology failure; business

premises becoming unavailable; inadequate document retention or record-keeping; poor management; lack of supervision, accountability and control; errors in financial models and reports; attempts to conceal losses or make personal gains (rogue trading); and third-party fraud.

Out-of-Band Communications: A way to send data (e.g., files) outside the context of normal communications. Out of band communications provide a secondary communications channel for emergencies and/or redundancy.

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Personal Digital Assistant (PDA): A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera

Personal Identification Number (PIN): A short sequence of digits used as a password.

Personnel: All COV employees, contractors, and subcontractors, both permanent and temporary.

Phishing: A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

Plain Text Message: A message sent without encryption.

Privacy: The rights and desires of an individual to limit the disclosure of individual information.

Privacy Officer: The privacy officer, if required by statute (such as HIPPA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Proprietary Information: Specific and unique material and information relating to or associated with a company's products, business, or activities. This information must have been developed for or by the company and must not be available freely from another source.

Recovery: Activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

Repudiation: Denial that one did or said something.

Residual Risk: The portion of risk that remains after security measures have been applied.

Restoration: Activities designed to return damaged facilities and equipment to an operational status.

Restricted Data: Data which has limited availability; based on COV regulations.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA): The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications.

Risk Mitigation: The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing IT security.

Recovery Time Objective (RTO): The amount of time targeted for the recovery of a business function or resource after a disaster occurs.

Secure: A state that complies with the level of security controls that have been determined to provide adequate protection against adverse contingencies.

Sensitive Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

Sensitive IT Systems: COV IT systems that store, process, or transmit sensitive data.

Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. Implied in this definition is the concept that no one person should have complete control. Separation of duties is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

Shared Accounts: A logon ID or account utilized by more than one entity.

Sign: The process of using a private key to generate a digital signature as a means of proving generation or approval of a message.

Signature: A quantity associated with a message that only someone with knowledge of a user's private key could have generated but which can be verified through knowledge of the user's public key.

Spyware: A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or

legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

State: See *Commonwealth of Virginia (COV).*

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System.*

System. See *Information Technology (IT) System*

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An Agency Manager responsible for the operation and maintenance of an Agency IT system.

Technology Strategy and Solutions (TSS): A directorate within VITA; the publisher of all VITA external and internal policies, standards, and guidelines. TSS develops architectural standards and the accompanying policies and procedures for the enterprise, and advises the CIO on architectural standards and exceptions. It also tracks emerging trends and best practices across the spectrum of technologies, including hardware, operating systems, networking and communications, security, and software applications.

Third-Party Provider: A company or individual that supplies IT equipment, systems, or services to COV Agencies.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token: A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Trojan horse: A malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. Trojan horse programs may look useful or interesting to an unsuspecting IT system user, but are actually harmful when executed.

Trusted: Recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

United States Computer Emergency Response Team (US-CERT): A partnership between the Department of Homeland security and the public and private sectors, intended to coordinate the response to IT security threats from the Internet. As such it releases information about current IT security issues, vulnerabilities and exploits as Cyber Security Alerts, and works with software vendors to create patches for IT security vulnerabilities. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *Incident Response Team.*

Universal Serial Bus (USB): A standard for connecting devices.

Untrusted: Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

USB Flash Drive: A small, lightweight, removable and rewritable data storage device.

User ID: A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

Virginia Department of Emergency Management (VDEM): A COV department that protects the lives and property of Virginia's citizens from emergencies and disasters by coordinating the state's emergency preparedness, mitigation, response, and recovery efforts

Version Control: A management process to traceability of updates to operating systems and supporting software.

Virus: See Malicious Code.

Virginia Information Technologies Agency (VITA): VITA is the consolidated, centralized IT organization for COV.

Vital Record: A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Workstation: A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.

9. IT SECURITY ACRONYMS

AITR: Agency Information Technology Representative

ANSI: American National Standards Institute

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan

COPPA: Children's Online Privacy Protection Act

COTS: Council on Technology Services

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Management Act

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

IRC: Incident Response Capability

ISA: Interconnection Security Agreement

ISO: Information Security Officer

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

OMB: Office of Management and Budget

PDA: Personal Digital Assistant

PIA: Privacy Impact Assessment

PII: Personally Identifiable Information

PIN: Personal Identification Number

RA: Risk Assessment

RBD: Risk-Based Decisions

RTO: Recovery Time Objective

SLA: Service Level Agreement

SDLC: Systems Development Life Cycle

SNMP: Simple Network Management Protocol

SOP: Standard Operating Procedure

SSID: Service Set Identifier

SSP: Security Program Plan

ST&E: Security Test & Evaluation

TSS: Technology Strategy and Solutions Directorate (VITA)

USCERT: Computer Emergency Response Team

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

Any Agency requesting an exception to any requirement of this policy and the related Standards must submit the form on the following page.

IT Security Policy & Standard Exception Request Form

Date of Request: _____

Requester: _____ Agency Name: _____

IT Security Policy or Standard to which an exception is requested:

_____

In each case, the Agency requesting the exception must

1. Provide the **Business or Technical Justification** for not implementing the Standard**:**

2. Describe the scope and extent of the exception:

3. Identify the safeguards to be implemented to mitigate risks associated with the exception:

4. Define the specific duration of the exception (not to exceed six (6) months):

Approved _____ _____
Agency Head Date

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____
Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date